量子符号の代数的構成法 (符号と暗号の代数的数理)

AUTHOR(S):

松本, 隆太郎

CITATION:

松本, 隆太郎. 量子符号の代数的構成法 (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 125-138

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25265

数理解析研究所講究録 1361 巻 2004 年 125-138

量子符号の代数的構成法

松本 隆太郎
東京工業大学 集積システム専攻
Ryutaroh Matsumoto
Dept. of Communications of Integrated Systems,
Tokyo Institute of Technology
Email: ryutaroh@rmatsumoto.org

2004年1月31日

概 要

量子通信の基礎となる量子力学を線形代数の知識だけを前提に解説した後, 量子誤り訂正符号の代数的構成法について解説する.

1 前書き

近年量子力学的な現象を利用することで, 計算や情報通信において古典力学の範囲内では実現できない現象を起こせることが知られて来た. 代表的な現象としてはディジタル情報 (ビット列) の交換だけで空間的に離れた二地点間で物理系の状態を瞬時に移す量子テレポーテーション [3], 従来の暗号のように安全性を計算量的な仮定に依存しない秘密鍵共有プロトコル [2], 従来の計算機では高速に解く方法が知られていない素因数分解問題を高速に解く量子アルゴリズム [15] などがある. これらの手法を実現するためには物理系の量子状態を雑音から保護する必要があるが, そのような保護を実現する手法が量子誤り訂正符号である. また量子誤り訂正符号は上記の量子鍵共有プロトコルの安全性の証明を与える上でも必要不可欠である [16]. 本稿では量子誤り訂正符号の概念を情報通信で用いる量子力学の基礎的な部分から解説する.

2 通信に使う量子力学

量子力学はある物理系に対して測定を行ったときに現れる測定結果の確率分布を計算する理論的な枠組である. 物理系には「状態」と呼ばれる概念があり, 状態

と測定の組合わせで測定結果の確率分布は定まる．物理系には複素ヒルベルト空間が対応する．通信への応用を考える場合ほぼ常に有限次元の複素ヒルベルト空間を取り扱う．有限次元の複素ヒルベルト空間は通常の内積付き複素線形空間なので数学的に難しい部分は少ない．

2.1 状態の記述

有限次元複素線形空間 $\mathcal{H}$ が対応する物理系の状態の中で，「純粋状態」と呼ばれる状態は $\mathcal{H}$ のノルム 1 の縦ベクトルで表される．またある純粋状態を表すベクトルをスカラー倍したベクトルは同じ状態に対応すると見做す．量子力学では純粋状態を表す縦ベクトルを $|\varphi\rangle$ のように $|$ と $\rangle$ を付けて記述する．また $|\varphi\rangle$ の双対ベクトルを $\langle\varphi|$ で記述する．純粋状態では無い一般の状態を混合状態と呼び，$\mathcal{H}$ 上のトレース 1 の半正定値行列で表され，純粋状態 $|\varphi\rangle$ は混合状態 $|\varphi\rangle\langle\varphi|$ で表される．

2.2 測定の記述

次に量子論に於ける測定について述べる．一般的な測定を完全に記述すると本稿のページ制限に収まらないので，射影測定と呼ばれる測定について説明する．一般的な測定の解説は例えば林の教科書 [7] などを参照されたい．ちなみに一般的な量子力学の教科書では射影測定しか説明されていない．今 m 個の値を取る測定が有ったとする．このとき各測定値が対応する $\mathcal{H}$ から $\mathcal{H}$ への線形写像 P_i が存在し

$$\begin{aligned} P_i^2 &= P_i, \\ P_iP_j &= 0\,(i \neq j), \\ \sum_{i=1}^{m} P_i &= I \end{aligned}$$

を満たす．物理系の状態が $\mathcal{H}$ 上のトレース 1 の半正定値行列 ρ で表されるとき，測定結果 i を得る確率は

$$\mathrm{Tr}[\rho P_i]$$

で表され，測定結果 i を得た後の物理系の状態は $P_i\rho P_i$ をトレース 1 に正規化した

$$\frac{P_i\rho P_i}{\mathrm{Tr}[P_i\rho P_i]} = \frac{P_i\rho P_i}{\mathrm{Tr}[\rho P_i]}$$

で表される．

ベクトル $|\varphi\rangle$ で表される純粋状態では測定結果 i を得る確率は $\|P_i|\varphi\rangle\|^2$ になり，測定結果 i を得た後の状態は $P_i|\varphi\rangle/\|P_i|\varphi\rangle\|$ となる．

一般の量子力学の教科書では測定を観測量を用いて表している. 観測量は $\mathcal{H}$ 上のエルミート行列 A で表される. 行列 A が

$$A = \sum_{i=1}^{m} \lambda_i P_i$$

とスペクトル分解されるとき ($\lambda_1, \ldots, \lambda_m$ に重複は無い), 観測量 A で表される測定は $\{P_1, \ldots, P_m\}$ で表される測定に対応する. 観測量 A を用いた測定では, 慣習的に測定結果 i を得ることを測定結果 λ_i を得ると言う.

2.3 状態の確率的な混合

ここで確率 p_j で状態 ρ_j にある系を測定することを考える. 測定結果 i を得る確率は

$$\sum_j p_j \mathrm{Tr}[\rho_j P_i] = \mathrm{Tr}\left[\left(\sum_j p_j \rho_j\right) P_i\right]$$

で与えられる. 従ってこの系の状態は $\sum_j p_j \rho_j$ にあると考えられる. また確率 p_j で状態 ρ_j にある系と状態 $\sum_j p_j \rho_j$ にある系を区別する手段は量子力学の枠組の中には無い.

2.4 測定の順番

系 $\mathcal{H}$ に $\{P_1, \ldots, P_m\}$ で記述される測定 P と $\{P'_1, \ldots, P'_n\}$ で記述される測定 P' を行うことを考える. 測定を行うと測定後の状態は測定前の状態から変わるので, P, P' という順番で測定を行う場合と P', P という順番で測定を行う場合では, 2回の測定結果の結合確率分布および2回の測定による状態変化は異なる. 測定結果の結合確率分布および測定による状態変化が測定の順番に依存しないための十分条件はすべての i, j について $P_i P'_j = P'_j P_i$ が成立することであることが素直な計算によって示せる. また2回の測定を2つの観測量によって記述している場合, 前述の十分条件は2つの観測量が作用素として可換であることと同値である.

2.5 状態の変化

物理系に対する決定的な (つまり確率的な曖昧さが無い) 操作は $\mathcal{H}$ 上のユニタリ作用素 U で表される. U で表される操作を混合状態 ρ にある系に行うと操作後の状態は $U\rho U^*$ になる. ここで U^* は U の随伴作用素である. また U で表される操作を純粋状態 $|\varphi\rangle$ にある系に行うと操作後の状態は $U|\varphi\rangle$ になる.

通信では入力に対して雑音のため出力が一意に定まらないので, 通信路を入力に対する出力の条件付き確率分布で記述する. 状態 ρ_{in} を送ったときの受信状態は確

率 p_i で受信状態 ρ_i が得られるとモデル化できる. しかしこのような受信状態の確率的な混合は $\sum_i p_i\rho_i$ で記述できる. 従って量子力学的な通信路は混合状態から混合状態への写像として記述できる.

通信路は状態の確率的な変化の一例だが, 決定的ではない一般の状態変化を表す写像 Γ はどのような性質を持つ必要があるだろうか? まず第一に確率的な混合 $p_1\rho_1 + p_2\rho_2$ に対する状態変化は $p_1\Gamma(\rho_1) + p_2\Gamma(\rho_2)$ にならなければ不自然である. 第二に行列のトレースを保存しなければ $\Gamma(\rho)$ が量子力学的な状態ではなくなってしまう. 第三に $\Gamma(\rho)$ は半正定値行列でなければならない. 第一と第三の条件を満たす写像は正写像と呼ばれるが, 実際には Γ は完全正写像と呼ばれるより強い条件を満たす写像で無ければならない. 完全正写像に関する説明は紙数の都合上割愛するが例えば [12, 7] などを参照して欲しい. 通信路の記述として完全正写像を用いればよいことを最初に指摘した研究者は Holevo [8] である.

ユニタリ作用素 U で記述される操作を完全正写像で記述した場合 $\Gamma(\rho) = U\rho U^*$ になる.

2.6 合成系の記述

複素線形空間 $\mathcal{H}_1$ で記述される系 1 と $\mathcal{H}_2$ で記述される系 2 が有ったとする. これら二つの系を合わせた合成系はどのように記述されるだろうか? まず合成系に対応する線形空間は $\mathcal{H}_1 \otimes \mathcal{H}_2$ になり, 今まで述べた状態, 測定, 状態の変化に関する記述はすべて合成系にも当てはまる. また系 1 だけにユニタリ作用素 U_1 で記述される操作を行い, 系 2 だけにユニタリ作用素 U_2 で記述される操作を行った場合, 合成系全体への操作は $U_1 \otimes U_2$ で記述される. 同様に系 1 だけに完全正写像 Γ_1 で記述される操作を行い, 系 2 だけに完全正写像 Γ_2 で記述される操作を行った場合, 合成系全体への操作は $\Gamma_1 \otimes \Gamma_2$ で記述される.

次に測定について述べる. 系 2 に影響を与えないように系 1 に $\{P_1, \ldots, P_m\}$ で記述される測定を行い系 1 に影響を与えないように系 2 に $\{Q_1, \ldots, Q_n\}$ で記述される測定を行った場合, 全体として測定は $\{P_i \otimes Q_j : i = 1, \ldots, m, j = 1, \ldots, n\}$ で記述される. 観測量を用いた用いた記述も同様で, 系 1 の観測量 A_1 を測定し系 2 の観測量 A_2 を測定することは全体として $A_1 \otimes A_2$ を測定することに等しい.

最後に合成系の状態について述べる. 系 1 が純粋状態 $|\varphi_1\rangle$ にあり系 2 が純粋状態 $|\varphi_2\rangle$ にある場合合成系の状態は純粋状態 $|\varphi_1\rangle \otimes |\varphi_2\rangle$ になる. しかし系 1 と系 2 の両方が純粋状態としては表せない混合状態 ρ_1, ρ_2 にある場合, 合成系の状態は $\rho_1 \otimes \rho_2$ になる場合もあるし成らない場合もある. このことについてはこの後述べる.

2.7 entangled 状態

系 1 の状態が ρ_1 で系 2 の状態が ρ_2 である場合合成系の状態は $\rho_1 \otimes \rho_2$ に必ずなるように思われるが, そうとは限らない. 例えば 2 つの系 $\mathcal{H}_1, \mathcal{H}_2$ がともに 2 次元で正規直交基底 $\{|0\rangle, |1\rangle\}$ を持ち, 合成系が純粋状態

$$\frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}$$

にあるとする. この状態は如何なる系 1 の混合状態 ρ_1 および系 2 の混合状態 ρ_2 を用いても $\rho_1 \otimes \rho_2$ と表せないことが素直な計算によって示せる. このように部分系の状態のテンソル積として表せない状態を entangled 状態と呼ぶ. それでは entangled 状態を部分系だけで見た場合どのような部分系の状態として表されるだろうか?

2.8 部分トレース

系 1 と系 2 からなる合成系の状態 ρ があり

$$\rho = \sum_{i=1}^{n} \rho_{1,i} \otimes \rho_{2,i}$$

と書けるとする. ここで $\rho_{1,i}$ は系 1 の状態空間の作用素であり, $\rho_{2,i}$ は系 2 の状態空間の作用素である. このような分解は常に可能である. この状態に対して系 1 だけに作用する測定 $\{P_1 \otimes I, \ldots, P_m \otimes I\}$ を行った後に測定結果 i を得る確率は

$$\begin{aligned}
\mathrm{Tr}\left[\left(\sum_{i=1}^{n} \rho_{1,i} \otimes \rho_{2,i}\right) P_i \otimes I\right] &= \mathrm{Tr}\left[\left(\sum_{i=1}^{n} \rho_{1,i} P_i\right) \otimes \rho_{2,i}\right] \\
&= \sum_{i=1}^{n} \mathrm{Tr}[\rho_{1,i} P_i] \cdot \mathrm{Tr}[\rho_{2,i}] \\
&= \mathrm{Tr}\left[\left(\sum_{i=1}^{n} \mathrm{Tr}[\rho_{2,i}] \rho_{1,i}\right) P_i\right]
\end{aligned}$$

このことから ρ を系 1 だけに注目した場合 $\sum_{i=1}^{n} \mathrm{Tr}[\rho_{2,i}]\rho_{1,i}$ という状態に見える. ρ からこのような系 1 の状態を得る操作を「系 2 上で部分トレースを取る」という.

3 量子誤り訂正符号の問題設定と目的

本小節の内容は図 1 で視覚的に要約されているので適宜参照していただきたい. 本稿では $\mathcal{H}$ は常に何らかの物理系に対応する p 次元複素線形空間とする. p は素数である. 量子誤り訂正符号の目的は k 個の物理系の任意の未知の状態 $|\varphi\rangle \in \mathcal{H}^{\otimes k}$ を雑音のある通信路を介して送ることである. 状態 $|\varphi\rangle$ をそのまま送ると雑音に

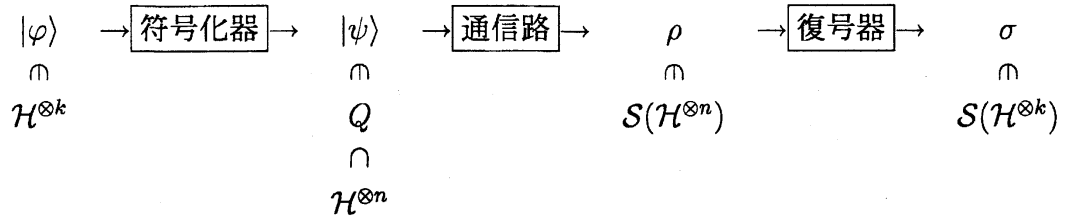

図 1: 量子誤り訂正の概念図: 純粋状態 $|\varphi\rangle$ を送りたい場合, まず符号化器により冗長性を付加する. 通信路を通って雑音が乗った状態 ρ を復号器でなるべく元の状態 $|\varphi\rangle$ に近い状態 σ に復元する. 但しここで $\mathcal{S}(\mathcal{H}^{\otimes n})$ は $\mathcal{H}^{\otimes n}$ 上の混合状態を表す.

よる変化を元に戻すことができないので, n 個の物理系の状態空間 $\mathcal{H}^{\otimes n}$ のある状態 $|\psi\rangle$ に $|\varphi\rangle$ を対応させて送る. この対応関係はユニタリ作用素で通常記述される. 従って送られる可能性のある符号語 $|\psi\rangle$ の集合は $\mathcal{H}^{\otimes n}$ の p^k 次元線形部分空間 Q に含まれる. この Q を符号空間と呼ぶ.

さて $|\psi\rangle$ を量子通信路を介して送り, $\mathcal{H}^{\otimes n}$ の混合状態 ρ が得られたとする. この状態 ρ を復号器で処理して状態 σ が得られたとする. 量子誤り訂正符号の目的は σ をなるべく $|\varphi\rangle$ に近くすることであるが, 量子状態は複素ベクトルまたは複素行列で表されある意味で連続的だから, 受信状態 σ が完全に送信状態 $|\varphi\rangle$ に一致することは稀である. そこで σ と $|\varphi\rangle$ の状態の近さを評価し, 状態が近ければ満足することにする.

このために状態の近さを評価する尺度が必要になるが, 量子誤り訂正符号で良く使われる尺度は Uhlmann [17] により提案され Jozsa [9] により様々な性質が明らかにされた忠実度 (fidelity) である. 純粋状態 $|\varphi\rangle$ と混合状態 σ の忠実度は

$$\langle\varphi|\sigma|\varphi\rangle \tag{1}$$

により定義される.

忠実度は以下のように解釈することができる. 観測量 $|\varphi\rangle\langle\varphi|$ を測定し結果 1 を得ることはある量子系が状態 $|\varphi\rangle$ にあるかどうか測定し系の状態が $|\varphi\rangle$ であるという結果を得ることに等しい. 忠実度 (1) は状態 σ にある系の観測量 $|\varphi\rangle\langle\varphi|$ を測定し結果 1 を得る確率に等しい. 従って σ が $|\varphi\rangle$ に近いほど忠実度が大きいと考えられる.

今までは純粋状態を送ることだけを考えて来たが, 前書きで述べた量子テレポーテーションなどに必要なエンタングルメントの共有ではエンタングルメントを構成する物理系の片方だけを送るので, 送信状態を $\mathcal{H}^{\otimes k}$ の純粋状態として表せない. しかし符号空間 Q の任意の純粋状態をある程度高い忠実度で送ることができる場合エンタングルメントを Q を用いて高い忠実度で送ることができることが知られているので [11], 純粋状態を送る場合に問題設定を限定しても差し支えない.

古典のブロック誤り訂正符号の性能評価は符号化率と最悪誤り確率によって行

うことが多いが, 量子誤り訂正符号も同様に符号化率 k/n と最悪忠実度

$$\min_{\substack{|\varphi\rangle\in\mathcal{H}^{\otimes k}\\ \langle\varphi|\varphi\rangle=1}} \langle\varphi|\sigma|\varphi\rangle$$

によって性能評価を行うことが多い. 次の節では符号の具体的な構成法について説明する.

4 量子誤り訂正符号 Q の構成法

この節ではCalderbankら [4, 5], Gottesman [6] らによって提案されたスタビライザー符号と呼ばれる量子誤り訂正符号の構成法を紹介する. この構成法は最も一般的な量子誤り訂正符号の構成法で, ほとんどの符号はこの構成法で得ることができる. また $\mathcal{H}$ の次元が 3 以上の場合への拡張はKnill [10] およびRains [14] による.

p 次元複素線形空間 $\mathcal{H}$ の正規直交基底 $\{|0\rangle, \ldots, |p-1\rangle\}$ を一つ固定する. λ を 1 の複素原始 p 乗根[1]とし, $p\times p$ 複素ユニタリー行列 C_p, D_λ を

$$\begin{aligned} C_p|i\rangle &= |i+1 \bmod p\rangle, \\ D_\lambda|i\rangle &= \lambda^i|i\rangle \end{aligned}$$

で定義する. $p=2$ のとき C_2, D_{-1} はPauli spin行列 σ_x, σ_z になることに注意せよ. ほとんどの量子誤り訂正の論文は $p=2$ の場合しか扱っていないが, $p=2$ の場合にしか興味が無い読者は $p=2$ と限定することにより補題1と2は容易に理解できるようになる. その他の部分は $p=2$ でも一般の場合でも理解の容易さは変わらない. C_p, D_λ は以下の性質を持つ.

補題 1 a, b, a', b' を整数とすると,

$$(C_p^a D_\lambda^b)(C_p^{a'} D_\lambda^{b'}) = \lambda^{a'b-ab'}(C_p^{a'} D_\lambda^{b'})(C_p^a D_\lambda^b).$$

証明: 定義より

$$\begin{aligned} (C_p^a D_\lambda^b)(C_p^{a'} D_\lambda^{b'})|i\rangle &= \lambda^{ib+ib'+a'b}|i+a+a' \bmod p\rangle, \\ (C_p^{a'} D_\lambda^{b'})(C_p^a D_\lambda^b)|i\rangle &= \lambda^{ib+ib'+ab'}|i+a+a' \bmod p\rangle \end{aligned}$$

を得る. これらの式を比較することにより補題の主張を確認できる. ■

補題 2 集合 $\{C_p^a D_\lambda^b : a=0,\ldots,p-1, b=0,\ldots,p-1\}$ は $p\times p$ 複素行列のなす線形空間の基底をなす.

[1] $\lambda^p=1$ かつすべての $j=1,\ldots,p-1$ について $\lambda^j\neq 1$ のとき λ を 1 の原始 p 乗根であると言う. 例えば $\exp(2\pi i/p)$ は 1 の原始 p 乗根である.

証明: $D_\lambda^0, \ldots, D_\lambda^{p-1}$ の対角成分を並べて作った行列はVandermonde行列なので, $D_\lambda^0, \ldots, D_\lambda^{p-1}$ の適当な線形結合で (j,j) 成分だけが 1 の $p \times p$ 行列を作ることができる. この行列に $C_p^{p+i-j \bmod p}$ を左から掛けると (i,j) 成分だけが 1 の行列を作ることができる. 従って $\{C_p^a D_\lambda^b : a = 0, \ldots, p-1, b = 0, \ldots, p-1\}$ の適当な線形結合で任意の $p \times p$ 複素行列を表すことが可能で, この集合の要素数は $p \times p$ 複素行列のなす線形空間の次元に等しいので補題を証明できた. ■

誤り群 $E = \{\lambda^i C_p^{a_1} D_\lambda^{b_1} \otimes \cdots \otimes C_p^{a_n} D_\lambda^{b_n} : a_1, \ldots, a_n, b_1, \ldots b_n, i$ は整数 $\}$, および E の可換部分群 S を考える. 補題1より集合 E は群演算に関して閉じている. ここで E は $\mathcal{H}^{\otimes n}$ に作用する線形変換 (行列) の集合だが, 群演算として線形変換の合成 (つまり行列の積) を考えている.

今後 S の固有空間として量子誤り訂正符号 Q を構成するが, その前に必要になる線形代数の事実を確認する. $p \times p$ 行列 A が対角化可能であるとは, $\mathbf{C}^p$ の基底 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_p\}$ で, 各々のベクトル $\boldsymbol{v}_i$ が固有ベクトルになっているものが存在することである. 対角化可能な $p \times p$ 行列 A, B に対し A と B が同時に対角化可能であるとは, $\mathbf{C}^p$ の基底 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_p\}$ で各々の $\boldsymbol{v}_i$ が A と B 両方の固有ベクトルになっているものが存在することを言う. もし A, B が対角化可能な $p \times p$ 行列で $AB = BA$ ならば, A と B は同時に対角化可能である. この段落で述べた事実の証明は例えば [1, Thm. 5, Chap. 1] に見つけることができる.

S は可換な行列のなす群なので, $\mathcal{H}^{\otimes n} = \mathbf{C}^{p^n}$ の基底 $B = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{p^n}\}$ で各々の $\boldsymbol{v}_i$ が S に属するすべての行列の固有ベクトルになっているものが存在する. $\boldsymbol{v}_i$ を基底 B に含まれる任意のベクトルとする. S の固有空間とは $\boldsymbol{v}_i$ を適当に選ぶことによって, 集合 $\{\boldsymbol{v} \in B : S$ に含まれるすべての行列 A について $\boldsymbol{v}$ と $\boldsymbol{v}_i$ は A の同じ固有値に属する $\}$ によって張られる線形空間としてえられる $\mathcal{H}^{\otimes n}$ の線形部分空間である. したがって1つの S の固有空間は S に属する各々の行列の属する固有値によって識別される. S は群であるので, S の固有空間を識別するには S の生成元になっている行列のどの固有値に属するかだけがわかれば十分である. 量子誤り訂正符号 Q を S の固有空間の1つとして構成する. 以下 Q の次元と訂正可能な誤りの数を検討する.

まず E に含まれる行列が Q に対してどのように作用するか検討する. E の要素はユニタリ行列なので, Q に属する状態を通信路を介して送ったときに生じるエラーと見做すことができる. $\mathcal{H}^{\otimes n}$ に含まれるベクトルを複素数倍しても同じ量子状態を表すので, S に含まれる行列は Q に含まれる量子状態に影響を与えない.

E の部分群 S' を

$$S' = \{A \in E : \forall B \in S,\ AB = BA\}$$

で定義する. 以下の補題により S' に含まれるエラーは検出できないことがわかる.

補題 3 $A \in E, |\varphi\rangle \in Q \setminus \{\mathbf{0}\}$ とすると, $A|\varphi\rangle \in Q \Longleftrightarrow A \in S'$ である.

証明: 最初に $A \in S' \Longrightarrow A|\varphi\rangle \in Q$ を証明する. 主張をを証明するためには, 任意の $B \in S$ に対し, $|\varphi\rangle$ と $A|\varphi\rangle$ が B の同じ固有値に属することを示せばよい. $|\varphi\rangle$

が B の固有値 η に属しているとする. $BA|\varphi\rangle = AB|\varphi\rangle = \eta A|\varphi\rangle$ より $A|\varphi\rangle$ も B の固有値 η に属する.

次に $A \notin S' \Longrightarrow A|\varphi\rangle \notin Q$ を証明する. $A \notin S'$ なので, 補題1より $BA = \tau AB$, $\tau \neq 1$ を満たす $B \in S$ が存在する. $|\varphi\rangle$ が B の固有値 η に属するとすると, $BA|\varphi\rangle = \tau AB|\varphi\rangle = \eta\tau A|\varphi\rangle$ より, $A|\varphi\rangle$ は $|\varphi\rangle$ と異なる B の固有値に属する. 従って $|\varphi\rangle \notin Q$. ■

補題 4 $A \in E$ に対し $AQ := \{A|\varphi\rangle : |\varphi\rangle \in Q\}$ と定義する. このとき AQ は S の固有空間である.

証明: $|\varphi\rangle \in Q$, $B \in S$, $B|\varphi\rangle = \eta|\varphi\rangle$ とすると補題を証明するには $A|\varphi\rangle$ の属する B の固有値が $|\varphi\rangle$ に依存しないことを示せばよいが, 補題1より $BA = \tau AB$ とすると $BA|\varphi\rangle = \tau AB|\varphi\rangle = \eta\tau A|\varphi\rangle$ より明らかである. ■

補題 5 S の固有空間からなる集合は $\{AQ : A \in E\}$ に等しい.

証明: $A \in E$ に対し $A|\varphi\rangle$ は S のどの行列に対しても固有ベクトルになるので, 集合 $\{AQ : A \in E\}$ は S の固有空間からなる集合に含まれることがわかる.

$|\varphi\rangle \in Q$ を非零なベクトルとする. 補題2とテンソル積の性質より, 集合 E は $p^n \times p^n$ 複素行列のなす線形空間を張る. 従って集合 $\{A|\varphi\rangle : A \in E\}$ は $\mathcal{H}^{\otimes n}$ を張る. 従って $\{AQ : A \in E\}$ は $\mathcal{H}^{\otimes n}$ の直交分解になっているので補題を証明できた. ■

次に剰余類群 E/S' を考えるために以下の補題を導入する.

補題 6 S' は E の正規部分群である.

証明: S' は 集合 $\{\lambda^i I : i$ は整数 $\}$ を含んでいる. 但しここで I は $\mathcal{H}^{\otimes n}$ の恒等写像である. $A \in E$, $B \in S'$ とすると, AB は剰余類 AS' に含まれる. $AB = \lambda^i BA$ とする. $\lambda^i IB \in S'$ なので $AB \in S'A$ である. ■

補題6より E/S' は群である. 補題3と補題4より群 E/S' の S の固有空間からなる集合への作用を定義することができる.

補題 7 $A_1S', A_2S' \in E/S'$ とする. もし $A_1S' \neq A_2S'$ ならば $(A_1S')Q \neq (A_2S')Q$ である.

証明: $A_3 = A_2A_1^{-1}$ とおくと $(A_1S')Q \neq (A_2S')Q \Longleftrightarrow Q \neq A_3Q$ である. 補題3と $A_3 \notin S'$ より $Q \neq A_3Q$ である. ■

定理 8

$$\dim Q = \frac{p^n}{\sharp(E/S')}.$$

但し $\sharp$ は集合の要素数を表す.

証明: 補題7と補題5より S の固有空間の数と E/S' の要素数が等しいことがわかる. 補題5より S の固有空間はすべて同じ次元を持つことがわかる. 従って $\dim Q = \dim \mathcal{H}^{\otimes n}/\sharp(E/S')$ である. ■

5 復号法

5.1 復号手続き

図1において符号化器の実現は概念的には自明であろう. ただ $|\varphi\rangle$ に補助的な系を付加してユニタリ作用素を作用させるだけである. この節では復号法について見ていく.

復号の概略は以下の通りである: 受信者は受信状態 ρ にある系を測定してどのような誤りが生じたのか推測する. 測定により状態 ρ は別の状態 ρ' に変化する. 次に受信者は推測した誤りの逆作用素を ρ' に作用させる. 逆作用素を作用させた状態を ρ'' とすると, もし誤りを比較的良く推測していれば ρ'' は送信状態 $|\psi\rangle$ に近いはずである. その後 ρ'' に対し符号化の逆を行って σ を得る.

上記の手続きでまだ明らかでない点はどのような測定を行うかということと, 測定結果から生じた誤りを推定する部分である. これらの点についてこれから解説する.

前節で符号構成に用いた可換群 S の固有空間の次元を p^k とする. このとき固有空間は全部で p^{n-k} 個あるのでそれらを $Q_1, \ldots, Q_{p^{n-k}}$ とする. $\mathcal{H}^{\otimes n}$ のベクトルを Q_i に射影する射影子を P_i とする. まず復号器は $\{P_1, \ldots, P_{p^{n-k}}\}$ で記述される測定を受信状態 ρ に行う. そうすると測定結果 i が得られ, 測定後の状態 ρ' は値域が Q_i に含まれる $\mathcal{H}^{\otimes n}$ 上の半正定値行列 (混合状態) になる.

この後送信状態 $|\psi\rangle$ は Q_1 の要素であったとする. また通信路の雑音 (誤り) として前節で定義した群 E の要素のうちどれかが生じたと仮定して復号操作を行う. そのような仮定の妥当性は後程検討する. 誤りとして有り得る要素の集合は $\{M \in E : MQ_1 = Q_i\}$ である. この集合の中で誤りとして最も尤もらしいものを通信路に関する統計的な知識を元にして決定する. 最も尤もらしい誤りを $M(i)$ とする. ここで $M(i)$ は測定結果 i の関数であることに注意する. そして測定後の受信状態 ρ' に $M(i)$ の逆を作用させ $M(i)^{-1}\rho' M(i)$ を得る. この状態 $M(i)^{-1}\rho' M(i)$ が図1の ρ'' に対応する. ρ'' に符号化操作の逆を行って送信状態 $|\varphi\rangle$ に近い状態 σ を得る. 符号の構成法より $M(i)S$ に含まれる誤りが生じたときにこの復号手続きで送信状態 $|\varphi\rangle$ を完全に復元できる.

以上の復号手続きから $\bigcup_{i=1}^{p^{n-k}} M(i)S$ に属するユニタリ行列が誤りとして生じた場合には完全に送信状態を復元できることがわかる. しかし実際に起きる誤りは $\bigcup_{i=1}^{p^{n-k}} M(i)S$ の要素として表せない場合がほとんどである. 3節で述べたように量子通信路は完全正写像を用いて記述される. 量子通信路の完全正写像から上に述べた復号手続きによる最悪忠実度の下界を評価する方法を次に述べる.

5.2 最悪忠実度の評価

量子通信路を記述する完全正写像とは大雑把に言えば $\mathcal{H}^{\otimes n}$ 上の混合状態の集合 $\mathcal{S}(\mathcal{H}^{\otimes n})$ からそれ自身への線形写像である. 通信路を記述する写像を $\Gamma_n : \mathcal{S}(\mathcal{H}^{\otimes n}) \to \mathcal{S}(\mathcal{H}^{\otimes n})$ とすると式 (2) で表されるように Γ_n は通信路と環境の相互作用の通信路の部分だけに注目したものと見なすことができる. ある p^{2n} 次元線形空間 $\mathcal{H}_n$, 長さ 1 のベクトル $|e_n\rangle \in \mathcal{H}_n$, $\mathcal{H}^{\otimes n} \otimes \mathcal{H}_n$ のユニタリ作用素 U_n が存在して

$$\Gamma_n(\rho) = \mathrm{Tr}_{\mathcal{H}_n}[U_n(\rho \otimes |e_n\rangle\langle e_n|)U_n^\dagger] \tag{2}$$

がすべての $\rho \in \mathcal{S}(\mathcal{H}^{\otimes n})$ について成り立つことが知られている. 但し $\mathrm{Tr}_{\mathcal{H}_n}$ は $\mathcal{H}_n$ 上の部分トレースを取ることを表している.

以上のような通信路の表現を用いて最悪忠実度の下界を求めることができる. $\mathcal{H}^{\otimes n}$ 上の線形作用素全体は線形空間をなすが, 集合 $\mathcal{B} = \{C_p^{a_1}D_\lambda^{b_1} \otimes \cdots \otimes C_p^{a_n}D_\lambda^{b_n} : a_1, \ldots, a_n, b_1, \ldots b_n = 0, \ldots, p-1\}$ はこの線形空間の基底になっている. 従って式 (2) の U_n を

$$U_n = \sum_{M \in \mathcal{B}} M \otimes L_M$$

と展開することができる. 但し L_M は $\mathcal{H}_n$ 上の線形作用素である. Preskill は [13] の 7.4 節で, $|\psi\rangle \in Q$ を送り復号後の状態が $\mathcal{H}^{\otimes n}$ の混合状態 ρ'' であったときの $|\psi\rangle$ と ρ'' の忠実度が

$$1 - \left\| \sum_{M \in \mathcal{B} \setminus \mathcal{B}_c} M|\psi\rangle \otimes L_M|e_n\rangle \right\|^2 \tag{3}$$

以上であることを明らかにしている. 但し $\mathcal{B}_c$ は $\mathcal{B}$ の中で訂正できる誤りの集合 $\mathcal{B} \cap \bigcup_{i=1}^{p^{n-k}} M(i)S$ である.

5.3 無記憶通信路と t 誤り訂正

古典の誤り率 p の二元対称通信路において符号長 n の二元線形ブロック符号を用いて誤り訂正を行う場合, もし t 個までの誤りを用いる符号が訂正できるならば正しく復号できる確率は

$$1 - \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

以上であることが良く知られている. このため二元対称通信路では誤り確率の代わりに訂正可能誤り数 t を符号の性能の指標として用いることができる. 量子誤り訂正符号においても, 同様に無記憶通信路と呼ばれる通信路のクラスでは訂正可能誤り数によって最悪忠実度の下界が定まることを紹介する.

通信路を表す完全正写像 $\Gamma_n : \mathcal{S}(\mathcal{H}^{\otimes n}) \to \mathcal{S}(\mathcal{H}^{\otimes n})$ がある $\mathcal{S}(\mathcal{H})$ の完全正写像 $\Gamma_1 : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ が存在して

$$\Gamma_n = \Gamma_1^{\otimes n}$$

と表せるならば, その通信路は無記憶であると言われる. また行列

$$M_1 \otimes M_2 \otimes \cdots \otimes M_n \in \mathcal{B}$$

の重みを $M_i \neq I$ であるような添え字 i の数とする. $\mathcal{B}$ の重みが t 以下の行列がすべて $\mathcal{B}_c$ に含まれるときに, 符号 Q は t 誤り訂正可能であると言う. 訂正可能誤り数 t と最悪忠実度の間には以下のような関係がある.

まず, ある p^2 次元線形空間 $\mathcal{H}_1$, $|e_1\rangle \in \mathcal{H}_1$, $\mathcal{H} \otimes \mathcal{H}_1$ 上のユニタリ作用素 U_1 を用いて

$$\Gamma_1(\rho) = \mathrm{Tr}_{\mathcal{H}_1}[U_1(\rho \otimes |e_1\rangle\langle e_1|)U_1^\dagger]$$

と Γ_1 を表す. 次に, $\{C_p^a D_\lambda^b : a, b = 0, \ldots, p-1\}$ は $\mathcal{H}$ の線形作用素からなる線形空間の基底をなすから, U_1 を

$$U_1 = \sum_{a,b=0,\ldots,p-1} C_p^a D_\lambda^b \otimes L_{a,b}$$

と展開することができる. 但し $L_{a,b}$ は $\mathcal{H}_1$ の線形作用素である. ここで

$$p = \sum_{a,b=0,\ldots,p-1,(a,b)\neq(0,0)} |L_{a,b}|e_1\rangle|$$

とおくと, $|\psi\rangle \in Q$ を送ったときの $|\psi\rangle$ と復号後の混合状態の間の忠実度は少なくとも

$$1 - \left[\sum_{i=t+1}^{n} \binom{n}{i} p^i\right]^2$$

であることが, 式 (3) から導くことができる.

参考文献

[1] L. E. Ballentine. *Quantum Mechanics: A Modern Development.* World Scientific, Singapore, 1998.

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Intl. Conf. on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar. 1993.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, Jan. 1997, quant-ph/9605005.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, July 1998, quant-ph/9608006.

[6] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54(3):1862–1868, Sept. 1996, quant-ph/9604038.

[7] 林 正人, "量子情報理論入門," サイエンス社SGCライブラリより出版予定.

[8] A. S. Holevo. On the mathematical theory of quantum communication channels. *Problems of Information Transmission*, 8(1):47–54, Mar. 1974. the original Russian article published in 1972.

[9] R. Jozsa. Fidelity for mixed quantum state. *J. Modern Opt.*, 41(12):2315–2323, 1994.

[10] E. Knill. Non-binary unitary error bases and quantum codes. `http://jp.arxiv.org/abs/quant-ph/9608048`, Aug. 1996.

[11] E. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, Feb. 1997, quant-ph/9604034.

[12] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[13] J. Preskill. Lecture notes for physics 229: Quantum information and computation, `http://www.theory.caltech.edu/people/preskill/ph229`, 1998.

[14] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, Sept. 1999, quant-ph/9703048.

[15] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997, quant-ph/9508027.

[16] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, July 2000, quant-ph/0003004.

[17] A. Uhlmann. The "transition probability" in the state space of a $*$-algebra. *Rep. Math. Phys.*, 9(2):273–279, Apr. 1976.